UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/758,865	01/16/2004	Raynold M. Kahn	PD-200289	8015

20991 7590 04/01/2008

THE DIRECTV GROUP, INC.
PATENT DOCKET ADMINISTRATION
CA / LA1 / A109
P O BOX 956
EL SEGUNDO, CA 90245-0956

EXAMINER	
ABRISHAMKAR, KAVEH	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
04/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/758,865	KAHN ET AL.	
	Examiner	Art Unit	
	KAVEH ABRISHAMKAR	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *18 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-18 and 28-31* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-18 and 28-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *2/15/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/18/2007 has been entered.

1. Claims 1-18, and 28-31 are currently being considered.

Response to Arguments

Applicant's arguments filed 12/28/2007 have been fully considered but they are not persuasive for the following reasons:

Regarding currently amended claims 1, and 10, the Applicant argues that the Cited Prior Art (CPA), Son et al. (U.S. Patent Pub. No. 2001/0017920) in view of Akiyama (U.S. Patent Pub. No. 2002/0001386), does not teach receiving encrypted program materials generated by a service provider at one or more of a plurality of networked receivers, wherein the networked receivers include at least one host receiver and at least one client receiver. This argument is not found persuasive. Son teaches that a broadcast source (service provider) sends encrypted broadcasts (encrypted program materials) to a distribution center (host receiver) and then the distribution center sends the broadcast to a plurality of subscriber stations (client receiver) (See

Figure 4). Son further teaches that it is conventional that there are one or more distribution centers, and a plurality of subscriber stations (paragraph 0020). Therefore, a plurality of distribution centers (host receivers) and a plurality of subscriber stations (client receivers) are present in the disclosure of Son. Therefore, it is respectfully asserted that the CPA does teach the above limitation, and the rejection is maintained as given below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record Son et al. (U.S. Patent Application Publication No~ 2001/0017920, hereinafter "Son")) and further in view of Akiyama (US 200200001386)

Claims 1, 10, parts A through part D are anticipated by Son et al., elements 502-516, figure 5B, where it. is understood that a "copy protection key" can be any key to decode the program material within the client/slave set top box (AKA integrated receiver/decoder). Paragraph 36 contains the detailed description of transferring both the copy protection key and the media to the client. Parts E and Fare anticipated by elements 518-522. Son teaches that a broadcast source (service provider) sends

encrypted broadcasts (encrypted program materials) to a distribution center (host receiver) and then the distribution center sends the broadcast to a plurality of subscriber stations (client receiver) (See Figure 4). Son further teaches that it is conventional that there are one or more distribution centers, and a plurality of subscriber stations (paragraph 0020). Therefore Son discloses a plurality of distribution centers (host receivers) and a plurality of subscriber stations (client receivers).

Son fails to teach c) means for encrypting the copy protection key at the host receiver using a host-client pairing key generated by the service provider and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the host-client pairing key for a particular combination the host and client receivers.

However, in an analogous art Akiyama teaches (paragraph 0099) a conditional access system when each receiver apparatus has an individual master key. Akiyama teaches that [paragraph 0100] the conditional access system adopts a key configuration, as shown in, e.g., FIG. 3. More specifically, a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see also paragraph 0101).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to employ the teachings of Akiyama into the method and

system of Son for encrypting the copy protection key at the host receiver using a host-client pairing key generated by the service prodder and shared between the host receiver and client receiver in order to share the program materials between the host receiver and client receiver, wherein the service provider establishes the laost-client pairing key for a particular combination the host and client receivers, in order to prevent cryptanalysis and huge transmission volume caused by periodic changing of the channel key (protection key) as suggested by Akiyama (paragraph 0100)

Claims 2, and 11 are anticipated by modified Son within paragraph 34. It is understood that a media decryption key refers only to the key that encrypted the media, and this is referred to as "A first key" within Son.

Claims 3, and 12 are taught by modified Son et al. within paragraphs 29 and 30, where it states that the host-client pairing key is received from the broadcast system on an "off air packet" transmission: "A first key.., may have been received from the video on- demand source 402 via a communication channel that is separate from the one used to transmit the video program. (Paragraph 29)." And, "The second key [...] itself may be transmitted from the remote server 404 to the subscriber station 110 while encrypted in a third encrypted form. (Paragraph 30)." It is apparent that both the "host'; and the "client" would receive said key.

Claims 4, and 13 are taught by modified Son within paragraph 29 and 30. It is inherent within the use of public key infrastructure (PKI, involving a public & private key set) that each key would be uniquely assigned to a device, whether it is the host or the client. Only within symmetric key cryptography is the keynot uniquely assigned.

Claims 5, 14 and 23 are taught by modified by Son within paragraph 36, where "...the remote server 404 responds by multiplexing the re-encrypted program in the second encrypted form (and the second key if necessary) with other signals to generate a multiplexed signal. (Paragraph 36)." This process is also done between the broadcaster and the server (or host receiver), as illustrated in Figure 5B. Thereby, both the host and client receivers would have to generate the "copy protection key" from the "content information" transferred thereto.

Claims 6-8, and 15-17 are taught by modified Son due to the inherency that content information involving content identification (based on the program materials) and copy control (otherwise known as Entitlement Management) encapsulated in what is typically known as Entitlement Management Messages is used to control the use of the program material in digital video broadcasting. Please see Wasilewski et al. (U.S. Patent No. 6,157,719) that shows inherency of EMM's within conditional access systems, and also see MPEP §2131.01.

Modified Son within paragraph 29 and 30 teaches claims 9, and 18. It is inherent within the use of public key infrastructure (PKI, involving a public & private key set) that each key would be uniquely assigned to a device, whether it is the host or the client. Only within symmetric key cryptography is the key not uniquely assigned to a device.

Claims 28-31, are taught by Son in view of Akiyama. Akiyama teaches (paragraph 0099) a conditional access system when each receiver apparatus has an individual master key (unique pairing). Akiyama teaches that [paragraph 0100] the

conditional access system adopts a key configuration, as shown in, e.g., FIG. 3. More specifically, a work key Kw (i.e. a pairing key) which is specified for each channel and is common to all receiver apparatuses (common to all receiver apparatuses) is encrypted using an individual master key KM, and the encrypted key is sent. Furthermore, a channel key Kch is encrypted using that work key Kw, and the encrypted key is sent (see also paragraph 0101).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Examiner, Art Unit 2131

/K. A./
3/25/08
Examiner, Art Unit 2131